IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, LLC, Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	Case No.: 2:18-cv-00094-EWH-LRL **PUBLIC VERSION - REDACTED**

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR ADDITIONAL AND AMENDED FINDINGS AND AMENDED JUDGMENT UNDER RULE 52(b) OR, IN THE ALTERNATIVE, FOR A NEW TRIAL UNDER RULE 59(a)(2)

TABLE OF CONTENTS

INTRODUCTION 1

PROCEDURAL BACKGROUND 2

ARGUMENT 3

I. THE '193 PATENT 4

A. The Court Adopted a Manifestly Erroneous Construction of "Particular Type of Data Transfer From [a] First Network to a Second Network" 5

1. The Switches and Routers Infringe Claims 18 and 19 of the '193 Patent if Properly Construed 5

2. At the Very Least, the Court Should Reopen the Judgment and Hold Additional Proceedings in Light of the New Claim Construction 9

B. The Court Misapprehended How Cisco's Switches and Routers Work 11

II. THE '806 PATENT 13

A. The Court Misapprehended Centripetal's Infringement Theory 15

B. The Court Erred in Construing the Claims' Requirement to "Cease Processing" Packets During a Rule Swap 19

C. The Court Improperly Compared the Accused Products to the Patent Specification, Rather Than to the Claims Themselves, Effectively Importing a Limitation Into the Claims 20

III. THE '176 PATENT 22

A. The Court Misapprehended How Received and Transmitted Packet Logs are Correlated 22

1. The Evidence Showed that Ingress and Egress NetFlow Records are Correlated by Stealthwatch 23

2. The Court Erred by Not Considering Certain Technologies that Correlate 25

3. The Court Improperly Compared the Specification of the '176 Patent to the Accused Products, Effectively Importing a Limitation Found Only in the Specification 27

B. The Court Erred in Concluding that the Accused Products Do Not Generate and Provision Rules in Response to Correlation 28

CONCLUSION..... 30

TABLE OF AUTHORITIES

Page(s)

Cases

Accent Packaging, Inc. v. Leggett & Platt, Inc.,
707 F.3d 1318 (Fed. Cir. 2013).....19

Becton Dickinson & Co. v. Tyco Healthcare Grp. LP,
No. Civ.A. 02-1694 GMS, 2006 WL 890995 (D. Del. Mar. 31, 2006).....9

Golden Blount, Inc. v. Robert H. Peterson Co.,
438 F.3d 1354 (Fed. Cir. 2006).....4

Haddad v. United States,
164 Fed. Cl. 28 (2023).....27

Merck & Co. v. Teva Pharms. USA, Inc.,
347 F.3d 1367 (Fed. Cir. 2003).....7

Morrow Corp. v. Harleysville Mut. Ins. Co.,
110 F. Supp. 2d 441 (E.D. Va. 2000).....4

Omega Eng'g, Inc. v. Raytek Corp.,
334 F.3d 1314 (Fed. Cir. 2003).....19

Pressure Prods. Med. Supplies, Inc. v. Greatbatch Ltd.,
599 F.3d 1308 (Fed. Cir. 2010).....9

SRI Int'l v. Matsushita Elec. Corp. of Am.,
775 F.2d 1107 (Fed. Cir. 1985).....20, 21

SuperGuide Corp. v. DirecTV Enters., Inc.,
358 F.3d 870 (Fed. Cir. 2004).....19

Thorner v. Sony Comput. Ent. Am. LLC,
669 F.3d 1362 (Fed. Cir. 2012).....6

Twigg v. Norton Co.,
894 F.2d 672 (4th Cir. 1990).....9

Wi-LAN, Inc. v. Apple, Inc.,
811 F.3d 455 (Fed. Cir. 2016).....9

Other Authorities

Fed. R. Civ. P. 52.....2, 7

Fed. R. Civ. P. 52(b) 1, 3, 4

Fed. R. Civ. P. 59 ..... *passim*

Fed. R. Civ. P. 59(a)(2) 1, 4, 13

Fed. R. Civ. P. 63 ..... *passim*

INTRODUCTION

Plaintiff Centripetal Networks, LLC ("Centripetal") recognizes that this case presented the Court with an unusual task. A district judge could spend a half-century on the bench and never find herself needing to pick up where another district judge left off—let alone needing to treat some of the initial judge's findings and conclusions as binding while disregarding others altogether pursuant to the mandate of a court of appeals. And even putting those procedural complications of Rule 63 aside (*see* Fed. R. Civ. P. 63), a district judge could spend decades without confronting a dispute as technologically complex as this one. The combination of the two—a highly technical patent lawsuit in which years of proceedings and thousands of pages of evidence and briefing were compiled and submitted before a different judge—made for a perfect storm. The Court sailed through many if not most of the issues this case presents expertly. But not all of them. The Court's ultimate conclusion that Defendant Cisco Systems, Inc. ("Cisco") did not infringe U.S. Patent Nos. 9,686,193 ("the '193 Patent"), 9,203,806 ("the '806 Patent"), and 9,560,176 ("the '176 Patent") rests on clear errors of fact and law that, if corrected, would compel a contrary conclusion. Centripetal thus respectfully moves to correct these errors and enter an amended judgment finding that Cisco infringes all three patents. *See* Fed. R. Civ. P. 52(b).

In the alternative, Centripetal respectfully requests that the Court reopen the judgment and receive additional testimony and argumentation on specific claim constructions and factual issues. *See* Fed. R. Civ. P. 59(a)(2). That may not be an ordinary remedy, but this was not an ordinary case. As a result of the Federal Circuit's limited vacatur and directive to employ Rule 63, the Court was left with a record spanning 3,500 pages, 26 witnesses, and more than 300 exhibits, all compiled before another judge. And although Centripetal determined on remand

that no supplementation was necessary, it did so on the understanding that the February 2020 claim construction order was not subject to vacatur. That understanding was driven not only by the Federal Circuit's opinion, which explicitly did not disturb any of the rulings made pre-trial (or even during trial), but also by the state of the case law: never before had a Rule 63 judge engaged in further claim construction that altered the settled understanding of the constructions reached by the initial presiding judge. Had Centripetal known that the Court intended to do so, it would not have certified that the case could proceed on remand without further record supplementation. Because the Court's decision depends on modifications to the scope of the asserted claims, *i.e.*, the plain and ordinary meaning, or new constructions that are either contrary to the specification or improperly limited to an embodiment in the specification, Centripetal respectfully submits that if the Court does not alter and amend the judgment under Rule 52 and conclude that Cisco's accused products are indeed infringing, the Court at the very least should reopen the judgment and allow the parties under Rule 59 to present additional evidence and briefing rebutting the new constructions underlying the non-infringement judgment.

PROCEDURAL BACKGROUND

The Court is obviously familiar with the case, so we provide only a brief overview. After years of litigation culminating in a 22-day bench trial, the late Judge Henry Coke Morgan issued a 167-page opinion concluding that Cisco willfully infringed the asserted claims of the '193, '806, and '176 Patents.[1] The Federal Circuit vacated that opinion without addressing or even hearing argument on the merits, holding that Judge Morgan needed to recuse once he learned on August 11, 2020, that his wife owned a small amount of Cisco stock. Dkt.646.

[1] Judge Morgan also found that Cisco willfully infringed Claims 24 and 25 of U.S. Patent No. 9,917,856; that patent is not a part of the present proceedings.

Because the stock-ownership issue was the only basis for its decision, the Federal Circuit remanded with instructions that rulings made *before* August 11, 2020—which includes Judge Morgan's claim construction order and all rulings he made during trial—were to remain intact. *Id.* at 26.

In light of the Federal Circuit's instructions, and relying upon the existing claim construction and trial record, Centripetal determined that no further supplementation of the record was necessary. Dkt.656. The Court later certified familiarity with the record under Rule 63 (Dkt.742), thus "determining that the case may be completed without prejudice to the parties" using the record compiled and rulings made by Judge Morgan. *See* Fed. R. Civ. P. 63.

At the Rule 63 hearing—which came eight months after Centripetal determined that no further record supplementation was necessary—the Court suggested for the first time that it might further construe the asserted patent claims beyond what had been settled in the pre-remand, non-vacated proceedings and depart from the plain and ordinary meaning of the claim terms. At that time, counsel for Centripetal explained the prejudicial impact of "changing the [claim construction] rules after the game is over." R.63 Tr. 432:22-439:15.[2] Ultimately, the Court issued new constructions that either were contrary to the plain and ordinary meaning and fundamental principles of claim construction, to find non-infringement in its Order (Dkt.780), as explained below.

ARGUMENT

Under Federal Rule of Civil Procedure 52(b), the Court "may amend its findings—or make additional findings—and may amend the judgment accordingly." The primary purpose of

[2] Citations to the Rule 63 hearing transcripts are referred to as "R.63 Tr." Citations to the 2020 trial transcripts are referred to as "Tr." Citations to the Court's Order (Dkt.780) are "Op."

a Rule 52(b) motion is to correct manifest errors of law or fact. *Morrow Corp. v. Harleysville Mut. Ins. Co.*, 110 F. Supp. 2d 441, 445 n.4 (E.D. Va. 2000). Rule 59(a)(2) similarly empowers the Court, following a bench trial, to "open the judgment . . . take additional testimony, amend findings of fact and conclusions of law or make new ones, and direct the entry of a new judgment." A party may move for amended or additional findings even if it would "in effect reverse the judgment." *Golden Blount, Inc. v. Robert H. Peterson Co.*, 438 F.3d 1354, 1358 (Fed. Cir. 2006) (citation omitted). "If the trial court has entered an erroneous judgment, it should correct it." *Id.* (citation omitted).

I. THE '193 PATENT

The '193 Patent discloses preventing cyberattacks in which a bad actor gains access to one or more computers within a network and then sends (*i.e.*, "exfiltrates") confidential data from the computer(s) in the network to a destination outside the network. *See* R.63 Tr. 107:5-16. Claims 18 and 19 recite applying "packet-filtering rules configured to prevent a particular type of data transfer from [a] first network to a second network." '193 Patent, 14:11-13, 46-49. If the transfer meets the criteria set forth in the rules—*e.g.*, if the packets are tagged and sent to a network associated with exfiltration risks—then the packets will be "dropped"; otherwise, they are conveyed to the destination network. *See id.* at 14:23-36, 14:56-15:2.

Cisco's Switches and Routers filter packets using a series of rules known as Access Control Lists ("ACLs"). Tr. 2550:5-7. They first apply ACLs that check the packet's destination, including whether the packets are being sent outside the network. *See* PTX-1288 at 012; PTX-1390 at 086. They then apply a Secure Group Access Control List ("SGACL") rule, which checks if the packet has been assigned a Security or Scalable Group Tag ("SGT") and, if so, forwards or drops the packet based on whether or not packets carrying that tag are allowed to

be sent to the contemplated destination network. *See id.*; Tr. 494:10-495:14. Cisco's Switches and Routers can isolate or "quarantine" computers in a network identified as a potential security risk, allowing them to communicate with certain network destinations but not others. *See* Tr. 524:14-526:7.

This Court's conclusion that the Switches and Routers do not infringe Claims 18 and 19 of the '193 Patent rests on a legally erroneous construction of key terms (which departed from the plain and ordinary meaning) and a misunderstanding of how the accused products function.

A. The Court Adopted a Manifestly Erroneous Construction of "Particular Type of Data Transfer From [a] First Network to a Second Network"

1. The Switches and Routers Infringe Claims 18 and 19 of the '193 Patent if Properly Construed

Centripetal respectfully submits that the Court's non-infringement decision rests on an erroneous construction of the asserted claims. Claims 18 and 19 of the '193 Patent disclose filtering a subset of data *transfers* between two different *networks*. '193 Patent, 14:11-13, 46-49. The Court construed the claims to "require … filtration of a subset of packets sent between *computers* in two different networks." Op.24 (emphasis added). Based on that construction, the Court required a showing that the accused products can drop "a subset or portion of the packets—either from a quarantined *computer* to a restricted destination or from a quarantined *computer* to a permitted destination" while forwarding "other packets to that same destination." Op.23 (emphasis added). But that is not what Claims 18 and 19 recite; nor would it make any sense for that to be what they describe, as switches and routers, typically cannot identify the specific computer where a given packet originated *at all* because the packet's origin information may be altered as it is transmitted (for example, if the packet travels through a proxy server). *See, e.g.*, R.63 Tr. 203:22-204:1. Instead, the claims' plain language describes filtration of a subset of data transfers from one *network* made up of many computers to *a second network*.

See '193 Patent, 14:11-13, 46-49. The distinction between those constructions—a transfer from Computer A to Computer B, versus a transfer from a network of computers on Network 1 to a network of computers on Network 2—may seem ephemeral, but it makes all the difference in the real world and in terms of how a person of ordinary skill in the art ("POSITA") would understand the claims and technology at issue.

"The words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art when read in the context of the specification and prosecution history." *Thorner v. Sony Comput. Ent. Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012). Here, because neither party proposed a construction, the parties agreed that the terms "particular type of data transfer" and "network" should be given their ordinary meanings. *See* Dkt.202. Right off the bat, then, the Court's claim construction is problematic because "computer" and "network" do not mean the same thing.

As a general matter, even laypeople understand that a computer is a single device that runs on or transmits data through a network, which is a group of interconnected devices. But the computer/network distinction is particularly important for the claims and technology at issue here. Experts from both sides agreed that a POSITA would understand that the type of "network" described in the claims generally comprises multiple separate computers. *See, e.g.*, R.63 Tr. 20:10-23 (Dr. Medvidovic testifying that, in a real network, "there would be thousands and thousands of each one of these devices, so lots of laptops, lots of printers, lots of servers"); R.63 Tr. 84:2-9 (Dr. Almeroth agrees); *see also* Op.11 (showing multiple devices within a network). It should therefore come as no surprise that both parties' experts agreed that the data transfers described in the claims refer to transfers of data packets between two *networks*, not transfers between just two *computers*. *See, e.g.*, Tr. 2400:8-10 (Cisco's expert stating that a

POSITA would understand that '193 Patent relates to "block[ing] some communication between the *two networks* but allow[ing] others communication to flow") (emphasis added); Tr. 490:17-491:2 (similar testimony from Centripetal's expert).

In collapsing that distinction, the Court seemed to assume that each network described in the claims contains just a single computer. Indeed, the Court ruled that embracing the claims' ordinary meaning, as Centripetal urged, would indicate that "the 'particular type of data transfer' would encompass *all* data transfers between the first network and the second network." Op.27. But the only way the "particular type of data transfer" would encompass all transfers from Network 1 to Network 2 would be if each network consisted of just one computer. The asserted claims of the '193 Patent, on their face, do not contain any one-computer-per-network requirement, and that is not how a POSITA would understand them.

In substituting "computer" for "network," the Court effectively read "from the first network to a second network" out of the claims—thus impermissibly rewriting them to recite a particular type of data transfer from one *computer* to a second *computer*. The Court's new construction improperly alters the plain and ordinary meaning of the claim element. That was manifest error and should be altered or amended pursuant to Rule 52.

Furthermore, the Court's new interpretation contravenes the settled rule that claims must be construed consistent with the patent specification. *See Merck & Co. v. Teva Pharms. USA, Inc.*, 347 F.3d 1367, 1371 (Fed. Cir. 2003). The '193 Patent specification describes data transfers between "network[s]" (of multiple computers each); it nowhere limits the claims to communications between two specific *computers*. For example, the specification describes how, in some embodiments, "[t]he filter may observe packets traversing the network link between the secured network and the unsecured network." '193 Patent, 2:6-11; *see also id.* at 6:41-46

(describing enforcing network policies to "restrict network communications between networks 104 and 106" pictured in Fig. 1). The Court's new construction is inconsistent with the claims' literal words, how experts would understand them, and the specification.

Adopting the correct construction of "particular type of data transfer from the first network to a second network" leads to a straightforward finding of infringement, as Cisco's Switches and Routers plainly block a subset of data *transfers* between two *networks*. There is no dispute that Cisco's Switches and Routers can block certain computers in the first network—namely those that have been assigned a "quarantine" SGT tag—from transferring packets to a second network. *See, e.g.*, Tr. 468:8-17 (a computer being used may reach some destinations, but not others, within an internal network); Tr. 489:22-490:16 (with exfiltration rules, a suspicious user may be restricted from accessing certain parts of an internal network but can otherwise continue to work). Further, Cisco does not dispute that its Switches and Routers can allow other computers in the first network (*i.e.*, those without the relevant SGT tag) to transfer packets to the second network. *See, e.g.*, Tr. 494:12-495:3 ("So if you've found a user that's suspicious you might say, okay, I'm going to apply this [SGT], in particular a quarantine tag."), 468:8-17, 489:22-490:16; PTX-1326 at 011 (change users' access privileges); PTX-563 at 414-415 (supplier's computer cannot access shared server in a second network); *see also* PTX-1280 at 0021 ("limit the endpoint's network access"). The Switches and Routers thus block a particular subset of data transfers from the first network to the second network, namely an exfiltration attempt from a quarantined computer identified by the presence of an SGT tag on the packet, as claimed in the '193 Patent. The Court should therefore enter an amended judgment of infringement of the '193 Patent.

2. At the Very Least, the Court Should Reopen the Judgment and Hold Additional Proceedings in Light of the New Claim Construction

If the Court nonetheless adheres to its new construction that the '193 Patent requires "filtration of a subset of packets sent between *computers* in two different networks," Op.24 (emphasis added), the Court at the very least should vacate and reopen the judgment to allow Centripetal the opportunity under Rule 59 to introduce evidence that Cisco's Switches and Routers infringe under the new construction the Court adopted, which was not advanced during trial. Claim construction guides assessments of infringement and validity, and the parties should be afforded the opportunity to address the constructions that the Court will be applying. Here, when Centripetal determined that no further record supplementation was necessary, it did not have notice of the Court's narrowed interpretation of the claims, which departed from the plain and ordinary meaning and thus prejudiced Centripetal. R.63 Tr. 432:22-439:15.

The Federal Circuit has been clear that rolling claim construction requires giving the parties sufficient notice and opportunity to present evidence and argument on the issue. *Compare, e.g.*, *Wi-LAN, Inc. v. Apple, Inc*., 811 F.3d 455, 464 (Fed. Cir. 2016) (district court erred in adopting new claim construction "at the JMOL stage"), *with, e.g.*, *Pressure Prods. Med. Supplies, Inc. v. Greatbatch Ltd*., 599 F.3d 1308, 1315-16 (Fed. Cir. 2010) (mid-trial claim construction change not prejudicial because district court provided "an *opportunity to consider the new construction and adjust its arguments to account for the change*") (emphasis added). Other courts have found similarly, awarding new trials under Rule 59 where a change in the court's theory caught the prejudiced party off-guard. *See, e.g.*, *Twigg v. Norton Co*., 894 F.2d 672, 675-76 (4th Cir. 1990) (new trial warranted where party lacked "opportunity to satisfactorily prepare to rebut" new theory of liability); *Becton Dickinson & Co. v. Tyco Healthcare Grp. LP*, No. Civ.A. 02-1694 GMS, 2006 WL 890995, at *12 & n.7 (D. Del. Mar.

31, 2006) (granting new trial where defendant "was unable to present expert testimony or properly respond otherwise" to new infringement theory).

That is exactly what happened here. Centripetal was not able to put on evidence at the Rule 63 proceeding, or even identify the need for new evidence until the Order came down. Under the constraints of the Rule 63 procedures, Centripetal was unfairly prejudiced and had no opportunity to address the Court's narrowed construction with evidence and witnesses. Centripetal properly raised at the Rule 63 Hearing that it would want to present new evidence through additional arguments and recalling witnesses if the Court adopted additional claim constructions. R.63 Tr. 437:6-24.

This was not harmless error. Had Centripetal known from the get-go on remand that the Court intended to narrow the claims, Centripetal would have insisted on introducing evidence that the Switches and Routers meet the construction of a "particular type of data transfer" as a subset of communications between computers in different networks. And Centripetal could easily have done so (and could do so if the Court were to reopen the judgment now under Rule 59), because the rules that the Switches and Routers employ may operate only on packets with a certain traffic type or payload information. For instance, Centripetal could show that the Switches and Routers use network segmentation, including microsegmentation, which limits traffic flows between specific computers across networks based on traffic types and application-layer information (which is in the payload of the packets). Declaration of Dr. Mitzenmacher ("Mitzenmacher Decl."), filed herewith, ¶¶ 4-6; PTX-1356 at .0001 (Microsegmentation with SGT); Mitzenmacher Decl., Ex. 1 at 1-2 ("Segmentation works by controlling how traffic flows among the parts. You could choose to stop all traffic in one part from reaching another, or you can limit the flow by traffic type, source, destination, and many other options . . . .

Microsegmentation uses much more information in segmentation policies like application-layer information."); *see also* R.63 Tr. 165:3-10 (Cisco website describes segmentation that can "limit the flow by traffic type, source, destination, and many other options"). Through network segmentation, the Switches and Routers provide security controls by limiting communications *between two computers* based on traffic type and application-layer information. Mitzenmacher Decl., ¶ 4.

This is not the only such evidence Centripetal could introduce showing that the Switches and Routers infringe under the construction the Court adopted. Thus, to the extent the Court maintains its claim construction and as a result of the peculiar procedural history of this case and the unique Rule 63 posture, the appropriate remedy under Rule 59 would be to vacate the non-infringement judgment on the '193 Patent and call for additional proceedings, whether in the form of additional discovery, additional testimony, and/or new briefing and argument.

B. The Court Misapprehended How Cisco's Switches and Routers Work

Separately, the Order rests on erroneous factual findings about the functionality of Cisco's Switches and Routers. In the Order, the Court viewed Cisco's filtering technology from the perspective of a quarantined computer—and, from that perspective, the Court's description of the technology is understandable. But the Switches and Routers function in such a way that they analyze the traffic between networks that contain a multitude of computers and the identification of the particular computer from which packets are sent can change as the traffic moves through the network.

The Court described the Switches and Routers as "devices [that] apply the quarantine SGACL rule and forward or drop the packet depending on whether it is destined for a restricted destination as specified by the ACL rules." Op.22. That description elides the complex series of operations that these devices perform. Cisco's Switches and Routers filter packets of data

traveling across networks of computers; when they receive a packet, they either "drop" the packet or forward it along toward a second or third network. *See, e.g.*, Tr. 21:8-23, 40:9-41:17. SGACL rules, which can drive the drop/no-drop decision, do not turn on the packet's destination alone; they also depend on the access privilege assigned to the packet, which is represented by the SGT value. That is important. Switches and Routers exist in a complicated network environment serving numerous endpoint computers—which means that they cannot readily determine the true source of a packet by examining the packet header (which may be altered during the packet's journey). This, in turn, is why the Switches and Routers must process the packet through a series of ACL rules, which includes checking the destination (*e.g.*, in the five-tuple of a packet), reviewing any SGT tag assigned to the packet (which indicates the role or the access privilege for that packet), and ultimately applying SGACLs. *See, e.g.*, PTX-1390 at 0086 (showing the application of various security ACL rules, determining access privileges with SGT value using GACL, and applying SGACL when the packet goes out); PTX-1280 at 021 (showing security group numbers and SGACL rules for that group).

Notably, application of the SGACL is the final step in this process; it occurs *after* the Switches and Routers already performed the destination check on the five-tuple. PTX-1390 at 0086. The point is that Cisco's Switches and Routers do, in fact, filter packets based on the particular type of data transfer at issue by *first* checking the five-tuple, reviewing SGT tags, and only *then* applying SGACLs. *See* Tr. 468:8-17, 489:22-490:16, 535:21-24. *Contra* Op.23.

Indeed, the Court's finding that SGACLs are only destination-based cannot be correct. If it were correct, then the SGACL would be entirely redundant in the packet processing flow; after all, before the SGACL is applied, the Switches and Routers already considered destination information for other types of ACLs, such as a router ACL ("RACL"). PTX-1390 at 0086; PTX-

1276 at 216. As explained, the Switches and Routers cannot effectuate a quarantine by performing a simple source and destination check, because they have limited visibility into the true source of a packet—meaning that Cisco's Switches and Routers do, in fact, filter packets based not only on the network destination, but also on the particular type of data transfer at issue. The Court should therefore amend its findings to conclude that the Switches and Routers satisfy the "particular type of data transfer" limitation of the '193 Patent and enter an amended judgment of infringement. Alternatively, in light of the peculiar procedural posture and the fact that the Court's findings were based in large part on a cold, paper record that was compiled in proceedings conducted by another judge, the Court should reopen the judgment under Rule 59(a)(2) to conduct further factfinding on this highly technical issue.

II. THE '806 PATENT

The '806 Patent describes systems by which network devices (*e.g.*, switches, routers, and firewalls) change the rule sets they apply, which has become vital as cyberthreats have grown dramatically and rapidly evolved. Claims 9 and 17 of the '806 Patent disclose a novel invention for quickly updating the rules by which network devices monitor and filter network traffic without any disruptions or outages. In "respons[e] to being signaled to process packets in accordance with [a] second [preprocessed] rule set," a network device "cease[s] processing of one or more packets; cache[s] [those] packets; [and] reconfigure[s] to process packets in accordance with the second rule set." '806 Patent, 11:41-46, 12:52-57. To address the evolving cyberthreat landscape, the rules that devices apply must be updated frequently; however, "the time required for switching between [rules] presents obstacles for effective implementation." '806 Patent, 1:13-21; Tr. 339:3-340:1.

In fact, Cisco faced this very problem. Cisco's earlier products dropped every incoming

packet while implementing new and old rules at the same time. *See* Tr. 597:13-598:9, 681:15-682:8, 3034:21-3035:15 (Cisco's old system caused packets to be dropped due to conflicts in the rules during a rule implementation); PTX-1195 at 3. In response to customer complaints, Cisco updated its product offerings to include the '806 Patent's technology. *See* Tr. 692:18-693:16; PTX-1196 at 6-7. Centripetal's '806 Patent solves the dropped-packets problem by ensuring that packets are only processed with one rule set at a time using new rule swapping technology that caches packets, instead of dropping them, while the actual rule swap occurs. *See* Tr. 572:19-573:7; '806 Patent, 4:60-64, 11:40-53, 1:41-52 (preprocessed rule sets can optimize performance). Cisco's accused products do the same.

Specifically, Centripetal accuses the following of infringing Claims 9 and 17 of the '806 Patent: (1) Switches or Routers, combined with Cisco's Digital Network Architecture ("DNA"), and (2) Cisco's Adaptive Security Appliances with Firepower services and Cisco's Firepower Appliances with Firepower Threat Defense (collectively, "Firewalls"), combined with Cisco's Firepower Management Center ("FMC"). Combination #1 (Switches and Routers plus DNA) updates rules using FED 2.0 Hitless ACL ("Hitless ACL"); Combination #2 (Firewalls plus FMC) similarly uses the Transactional-Commit Model. PTX-1195 (referring to FED 2.0 Hitless ACL); PTX-1293 at 668-669 (describing the Transactional-Commit Model); Tr. 596:20-597:11, 680:1-682:8. DNA and FMC collect rules and preprocess rule sets, which they then send to the relevant accused network devices (Switches, Routers, and Firewalls). These accused network devices initially process packets using one rule set and then, when signaled, stop processing the packets with those rules; they then cache incoming packets and swap to a second rule set. Tr. 600:6-603:17, 680:1-681:10, 684:16-686:23. Upon receiving another signal indicating that the rule swap has been completed, the accused network devices begin processing the packets using the new rules.

Id. In other words, the accused network devices do exactly what Claims 9 and 17 of the '806 Patent describe.

The Court's analysis of the '806 Patent contains three distinct errors. The Court (1) misunderstood how Cisco's accused products cause a network device to stop processing and cache packets during a rule swap, and thus, mistook Centripetal's infringement case; (2) misconstrued the claims' requirement to "cease processing" packets during a rule swap; and (3) improperly compared the accused products to ancillary benefits described in the patent specification, rather than the asserted claims themselves. Separately and together, these errors justify amending the judgment of non-infringement, or at least reopening discovery and holding further proceedings.

A. The Court Misapprehended Centripetal's Infringement Theory

The Court's non-infringement finding for the '806 Patent rests on erroneous factual findings about how the accused products work and the evidence in the record. In the Order, the Court did not address what Centripetal actually pointed to for infringement of the '806 Patent. Centripetal asserted that the accused network devices stop processing packets with the old rule set and cache those packets *while it completes the rule swap* (which is what Claims 9 and 17 of the '806 Patent describe). Yet the Court assessed how the accused network devices behave *during normal packet processing* (*i.e.*, when no rule swap is happening). The Court observed that the accused network devices "cease processing packets" during an extremely brief "idle period" and "use a form of a queue or buffer to store packets," all of which occurs during normal packet processing. Op.37, 40. The idle period, which are the two to four clock cycles between processing of each packet, exists in the normal processing of packets.

When a device gets a signal for a rule swap, however, the rule swap will change the normal processing of packets and take advantage of the clock cycles during the "idle" period to

introduce the new rule swapping functionality. The rule swap process thus causes different actions to take place than what otherwise would have occurred during normal packet processing. Since there are no rules to be applied while rules are being swapped, there is no processing of any packets during this time. Tr. 616:15-617:18. That is undisputed: Cisco's engineer, Mr. Jones, agreed that the Switches and Routers do not subject packets to any rules during a rule swap. *See* PTX-1915 (stating that no packets are "subject to rules" during a rule swap); *see also* Tr. 606:6-608:9 (Dr. Mitzenmacher confirming Mr. Jones' testimony that Hitless ACL design is not to allow packets through during a rule swap); *see also* Tr. 841:8-22 ([redacted] The Firewalls also cannot process packets during rule swapping, because the memory is being used to change the rule sets. *See* Tr. 704:23-705:10 ("During that time you can't be processing packets, right? Because you're actually trying to move, swap things in and out of memory.").

That is why Centripetal has consistently alleged that the step in which the accused network devices verify the existence of Hitless ACL (or equivalent) functionality—shown as "Step 7" in PTX-1195—provides the requisite "signal[]" to perform a rule swap.[3] PTX-1195 at 4. Centripetal supported this allegation with expert testimony, Cisco's own documents, and source code showing that the signal in Step 7 triggers a special rule-swapping process that interrupts normal packet processing. *See, e.g.*, Tr. 616:15-617:18 ("So the first signal, you have to say, okay, everything is ready to go into the hardware [*i.e.*, the TCAM]. Now I wait and stop

[3] [redacted]

and then implement the swap"); PTX-1195 at 4 (Step 7: "Verify if feature supports hitless[sic] ACL change"); *see also* Tr. 602:5-19, 615:17-24. In other words, in response to the initial signal, the accused network devices switch states from normal packet processing to a rule-swapping state during which they cache packets (to avoid dropping them), switch the rule sets, and signal that the swap is complete—just as the asserted claims describe. *See* PTX-1195 at 4; Tr. 616:15-620:16 (describing the steps), 631:25-632:9 (describing "success" as finishing the swap), 600:6-603:17 (describing the replacement of rules in TCAM); *see also* Tr. 680:11-682:8, 697:8-698:2 (Dr. Mitzenmacher describing the signal for Firewalls to swap rule sets to cease processing packets and cache incoming packets), 701:16-707:1 (describing ceasing processing and caching for under Transactional-Commit Model).

In response to the signal in Step 7, if the Hitless ACL technology is enabled, the processor will monitor the state of the packet analysis to ensure that the current packet has finished processing in order to avoid the old regime which would apply new rules instantly and cause packets to drop because of a conflict in the rules being applied. *See* Tr. 597:13-598:9, 681:15-682:8, 3034:21-3035:15 (Cisco's old system caused packets to be dropped due to conflicts in the rules during rule implementation); PTX-1195 at 3-4. Using Hitless ACL, once processing of that packet is complete, the processor will stop processing of all further packets and enter a state in which no rules are applied to any packet. This state of the rule swap process, where no rules are available in memory to be applied to any packets, meets the cease processing limitation. Notably, this state of the processor did not exist without Hitless ACL because the because rules were constantly applied to packets, even if they overlapped, and the packets were simply marked to be dropped rather than preserved in a cache.

The Court identified in its Order the moment that the rules are swapped, where it states

that there is a switch of rules which "occurs during the time between the firewall's processing of individual packets." Op.36. This interruption of normal packet processing meets the "cease processing" of packets element.

Centripetal showed further that the signal to switch rule sets causes the accused network devices to cache packets, just as the asserted claims describe. [redacted] Thus, in the accused network devices, processing pursuant to the old rule set ceases in response to a signal, and packets are then preserved in a cache (rather than dropped) while the new rule set are loaded. That is exactly what Claims 9 and 17 of the '806 Patent describe.

By focusing on "idle" time during normal processing rather than on what occurs during the rule swap process, the Court mistook Centripetal's infringement case. The Court erroneously concluded that the accused products are non-infringing and therefore committed a manifest error of law. That error is clear in the record, but to the extent the Court is uncertain in light of the foregoing, the proper remedy would be to reopen the judgment and, pursuant to Rule 59, provide

the parties additional opportunities to present evidence on this issue and/or present briefing and argument.

B. The Court Erred in Construing the Claims' Requirement to "Cease Processing" Packets During a Rule Swap

In addition to misunderstanding Centripetal's allegations, the Court appeared to misconstrue Claims 9 and 17 of the '806 Patent in concluding, contrary to the intrinsic evidence, that "cease processing of one or more packets" does not mean stop processing with the old rule set. *See* Op.41-44; *see also Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d 1318, 1326 (Fed. Cir. 2013) ("[A] claim interpretation that excludes a preferred embodiment from the scope of the claim is rarely, if ever, correct.") (citation omitted).

The specification explicitly states that "ceasing to process packets" occurs "when a current packet has been examined against the rules in policy 130's rule set [*i.e.*, first rule set]" and the processor stops *to switch rule sets*. '806 Patent, 8:4-23; *id.* at 6:12-15 (describing swapping rule sets in between processing packets); *id.* at 7:25-32, 7:57-59 (describing processing a packet with the first rule set, waiting until completion, and processing the next packet with the second rule set). In other words, it identifies in plain terms that "ceasing to process packets" is synonymous with "stop processing packets *with the old rule set*." Bringing the point home, there is no evidence in the record of any disclaimer by the patent applicant that would justify ignoring such a description of the invention in the specification. *See Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1323-28 (Fed. Cir. 2003) (terms should be given their full and ordinary meaning unless there is clear and unmistakable disavowal of claim scope).

The Court's construction also depends on improperly treating an embodiment in the specification (Figure 4) as a limitation on the claims. *See SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) ("The written description . . . is not a substitute for, nor

can it be used to rewrite, the chosen claim language."). Contrary to the Court's stated understanding, Figure 4 does not indicate that the claim requires "ceasing processing of packets altogether, not just with the old rule set." Op.42-44. In fact, it makes clear that the opposite is true: at Step 404 ("cease processing packets"), "each of processors 300, 302, and 304 may cease processing packets *in accordance with [the old] rule set*." '806 Patent, 9:4-8 (emphasis added). Thus, Figure 4 undermines the Court's construction and instead supports Centripetal's reading that the claims only require ceasing processing with the old rule set.

Again, Centripetal had no notice of the Court's interpretation of this claim limitation, which contradicts the specification, and Centripetal thus lacked an opportunity to brief the Court and address the new construction with additional evidence during the Rule 63 proceeding. The Court should thus amend the judgment to find infringement, or at the very least reopen the judgment to permit additional discovery, new testimony, and/or new briefing and argument.

C. The Court Improperly Compared the Accused Products to the Patent Specification, Rather Than to the Claims Themselves, Effectively Importing a Limitation Into the Claims

It is black-letter law that patent infringement "is determined by comparing an accused product" with the asserted patent claims, "not with a preferred embodiment described in the specification." *SRI Int'l v. Matsushita Elec. Corp. of Am.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985). After all, "claims are infringed, not specifications." *Id.* In analyzing the '806 Patent, however, the Court committed legal error by comparing Cisco's accused products to the specification. The specification states that "processing packets in accordance with an outdated rule set" may "exacerbate rather than mitigate the impetus for the rule set switch." '806 Patent, 1:25-31. And the Court found that Cisco's accused products do not infringe the '806 Patent because they continue to "process[] packets with an outdated rule set" while configuring a new rule set. Op.44. But that is not the right comparison. The only issue for infringement is whether the

accused products meet *the claims*; whether they meet *the specification* is irrelevant. *See SRI Int'l*, 775 F.2d at 1121-22 (comparing accused device against specification rather than claims was reversible legal error).

In any event, the specification's passing reference to "outdated rule sets"[4] during a rule implementation does not limit the scope of the invention and discusses the old regime in which old and new rules overlapped. The specification simply notes—in a single sentence in the two-paragraph "Background" section—that processing with an outdated rule set *may* be a negative in "certain circumstances." '806 Patent, 1:19-31. Moreover, the specification discusses "implementing a new rule set" while "continuing to processes packets" with "an outdated rule set," which is the old regime that causes a conflict of rules and results in the dropping of packets. *Id.* Furthermore, when the Court cited Mr. Shankar's testimony that Firewalls use old rules to process packets because it uses "outdated rule sets," Op.44 (citing Tr. 2518:22-2519:7), the Court misinterpreted what he was referring to. This testimony describes what occurs during normal packet processing *before* any signal to swap rules has been sent. This period satisfies a different part of the asserted patent claim, namely, the processing of packets under the first rule set. It simply is not relevant to the portion of the claims that invokes a rule swap and processing *under the second rule set*. Mr. Shankar's testimony is thus not evidence of non-infringement.

In sum, the Court's analysis of the '806 Patent rests on several manifest errors of fact and

[4] Cisco misdirected the Court by asserting that the '806 Patent is only about not using an outdated ruleset on a handful of packets received during a rule swap. That is simply an additional benefit, but not the sole purpose. In fact, the "outdated rule sets" is a secondary problem and is described in the specification exactly that way: "*Additionally*, while implementing a new rule set, a network protection device may continue processing packets in accordance with an outdated rule set." '806 Patent, 1:19-31 (emphasis added). The very first problem described in the background is avoiding outages that would result in dropped packets. *Id.*

law that, if corrected, require an amended judgment of infringement. Alternatively, the Court should reopen the judgment under Rule 59 and take additional testimony on these issues.

III. THE '176 PATENT

The '176 Patent analyzes and correlates logs corresponding to network traffic to identify and remediate unusual activity using network security rules. '176 Patent, 1:36-50; Tr. 973:16-974:22. The claimed "correlation" system of the '176 Patent "generate[s] . . . log entries corresponding to . . . packets received by" and "transmitted by the network device," uses those logs to "correlate" the transmitted and received packets, and uses the results to "generate and "provision" appropriate network rules. '176 Patent, 17:6-35, 18:63-19:23. These rules can block packets from an infected computer.

Cisco's Switches and Routers combined with Stealthwatch infringe Claims 11 and 21 of the '176 Patent because of their ability to analyze network traffic to identify an infected computer. Cisco's Switches and Routers collect data on the packets they see and send the data to Stealthwatch for analysis. Tr. 975:17-976:9, 984:19-24. Stealthwatch receives this data, correlates the data together to deduplicate the packet information, and identifies computers in the network that may be infected. R.63 Tr. 146:1-16 (Cisco's expert confirming the collection of both ingress and egress NetFlow records.); Tr. 994:21-995:8; PTX-1065 at .0005; *see also* R.63 Tr. 177:14-178:1; PTX-569 at 271. Stealthwatch can then prepare a policy update to prevent the computer from infecting other computers. Tr. 1002:11-1003:1. The Court erred by finding that these accused products neither correlate data related to received and transmitted packets nor generate and provision rules.

A. The Court Misapprehended How Received and Transmitted Packet Logs are Correlated

Undisputed evidence confirms that the accused products do in fact correlate data for

packets received with data for packets transmitted. *Contra* Op.56-59.

1. The Evidence Showed that Ingress and Egress NetFlow Records are Correlated by Stealthwatch

It is undisputed that Cisco's Switches and Routers are able to generate and process ingress and egress NetFlow records and send them to Stealthwatch for correlation. Tr. 988:12-992:5; PTX-572 at 762; PTX-569 at 272; PTX-1849 at 243. Dr. Cole demonstrated—using Cisco's own documents—that Stealthwatch may be used to compare ingress NetFlow records with egress NetFlow records. Tr. 993:19-999:15. Further, an internal Cisco presentation described how the collected NetFlow records are analyzed and correlated to identify threats. Tr. 994:12-995:21; PTX-1065 at .0005. Additional documentation showed that NetFlow records specifically were correlated, which, as construed in the *Markman* order, requires comparing log entries for received packets with log entries for transmitted packet. Dkt.202 at 17-19 (construing "correlate, based on the plurality of log entries," to mean "packet correlator may compare data in one or more log entries with data in one or more other log entries"); *see, e.g.*, PTX-591 at 522 (stating that Stealthwatch will collect NetFlow and WebFlow telemetry and correlate "both telemetry types"); PTX-1009 at .0009 (similar); PTX-1060 at .0023 (listing Stealthwatch's ability to collect and analyze 192,000 ingress and 192,000 egress entries, thus showing that both ingress and egress records are collected and correlated); *see also* Tr. 1108:6-18, 1116:14-1117:1 (Dr. Cole confirming that ingress and egress NetFlow records are correlated).

In light of this evidence, the Court erred in concluding that Centripetal failed to establish that ingress and egress NetFlow records are correlated. The evidence the Court cited in its Order does not refute that Cisco's technology permits correlation of ingress and egress NetFlow records. Rather, it shows, at most, that using both types of data may cause a miscounting of packets for traffic statistics and that users have the option of choosing to ignore egress records.

This alleged miscounting is a red herring because the functionality to correlate NetFlow records still exists in the product and the traffic statistics are not relevant to Dr. Cole's infringement analysis. Moreover, the user manual on which the Court relied (PTX-569) does not indicate that ingress and egress records cannot be correlated because the manual only states that a miscounting of traffic statistics may occur if both are provided.[5] PTX-569 at 282 ("For devices that use logical interfaces enabling both [ingress and egress] may cause the Flow Collector to double report traffic stats in non-interface documents. We usually ask the Customer to choose which data set is most important."). This excerpt also shows that double reporting occurs only when ingress and egress NetFlow records are collected for a single "logical interface." Cisco's own expert testified that ingress and egress data are collected on multiple interfaces, *see, e.g.*, Tr. 2283:6-18, in which case the alleged double-reporting problem does not occur.

[redacted]

[5] Cisco's expert erroneously calls this miscounting an "error condition," but there is no support that any actual error occurs that would prevent or disrupt correlation. R.63 Tr. 135:18-24. Mr. Llewallyn did not use this term and it does not appear in any of the documents. Rather, this was a term created without support by Cisco's expert, Dr. Almeroth.

[redacted] Thus, by default, Stealthwatch uses both ingress and egress during correlation.

Mr. Llewallyn's testimony likewise does not support the Court's finding that ingress NetFlow records are not compared to egress NetFlow records because the claims do not require that the data be explicitly marked as ingress or egress data when processed by Stealthwatch. The Court concluded that there is no comparison because "even if both ingress and egress records were collected by Stealthwatch, that distinction is lost before any correlation could occur." Op.58. However, the claims only require the correlation of received and transmitted packet data; they do not require the accused products maintain a separate ingress/egress "distinction" during comparison. Thus, Mr. Llewallyn's testimony does not support the Court's ruling.

2. The Court Erred by Not Considering Certain Technologies that Correlate

The Court also erred by failing to consider that the accused products correlate data when they deduplicate data flows. PTX-569 at 271 (confirming that Stealthwatch performed deduplication). Cisco's expert conceded that deduplication is a process where ingress and egress NetFlow records are compared to identify identical flows. R.63 Tr. 177:14-178:1 (Dr. Almeroth confirms that during deduplication, ingress and egress flows are compared and deduplicated). The comparison of NetFlow records for ingress and egress for deduplication meets the Court's claim construction that they are correlated.[6] The Court should amend its Order to address the deduplication functionality or, alternatively, hold additional proceedings (under Rule 59) in

[6] While the claims allow for more than one "network device," this deduplication process does not require more than one "network device," but instead involves collected NetFlow records from more than one Switch or Router placed before and after a single network device—such as a server or other network component. *See* '176 Patent, 2:58-61. As Mr. Llewallyn stated, these NetFlow records are almost always collected from multiple Switches and Routers for correlation. Tr. 2149:13-18.

which the parties may further address this functionality.

The Court also erred in concluding that Centripetal's sole infringement theory was based on NetFlow records. Op.55-56; Dkt.725 (Centripetal FoF/CoL) at ¶¶ 54 (CoL), 351-352 (FoF). Centripetal asserted infringement of the '176 Patent based on different types of "log entries," which, when correlated together, can be used to create rules. Tr. 998:6-999:5. Centripetal identified evidence that this additional data could be used with the NetFlow records for the correlation. Tr. 994:12-995:21; PTX-1065 at .0005 (showing web proxy data); PTX-591 at 522. The Court erroneously did not consider whether proxy data, in conjunction with NetFlow records, infringes. This is important because proxy data is also generated for packets that are received and transmitted, and proxy data is also compared with NetFlow records.

Further, the evidence the Court cited does not refute the relevance of these theories. Op.55-56. Rather, it shows that NetFlow records by themselves infringe, and also that the inclusion of additional data could be used to infringe. For example, the Court relied on Dr. Cole's statement that "the important thing for me are the ingress and egress NetFlow data. There's nothing in the claim that's exclusive to just those two, so there can be other data in there as long as those two NetFlow records are being correlated." Tr. 1108:1-5. When this quote is taken in the context of the earlier questions, it shows that proxy data is also sent along with the NetFlow ingress and egress records, and that combination also infringes. Tr. 1107:6-14. While Dr. Cole noted the infringement scenario where ingress and egress NetFlow records were correlated, he also relied on theories involving other proxy data. Tr. 1109:7-19, 1115:2-1116:20. Using this proxy data is relevant to the Court's conclusion because the data from NetFlow and WebFlow are for different packets, and any argument about ignoring egress packets is irrelevant because there is no double counting of packets. The Court's other citations similarly discuss the

infringement theory for the NetFlow records, but do not address Centripetal's other theories.

The Court's reliance on statements made by Centripetal's counsel during the Rule 63 hearing likewise do not support that Centripetal only alleged infringement based on NetFlow records. *See* Op.55-56. Reading the entire set of questions from the Court shows that the discussion was only about the use of NetFlow records, and Centripetal's counsel stated, "[w]e may have alternative theories. We may have syslog, and we have other stuff." R.63 Tr. 482:12-13. This statement establishes that data from the proxy, such as Syslog, was an alternative theory where proxy data augmented NetFlow records. The Court erred by failing to address this theory.

3. The Court Improperly Compared the Specification of the '176 Patent to the Accused Products, Effectively Importing a Limitation Found Only in the Specification

The Court also erred in its analysis of the "correlate" element because the Court compared the accused products to the discussion of packet obfuscation in the patent specification rather than applying the asserted claims. Op.59. As discussed above, this is not the correct analysis. *See supra* Part II.C. The Court asserted that Cisco's accused products do not infringe because they do not solve "the problem that the'176 Patent was designed to solve—packet obfuscation by a network device." Op.59. However, it appears the Court was comparing the products to the specification rather than the claims. *See* '176 Patent, Claims 11, 21.

While the '176 Patent does state that network devices altering the flow of a packet is a problem it can address, *see* '176 Patent, 1:21-25, Cisco is not entitled to a non-infringement defense based on the embodiments described in the specification. '176 Patent, 13:63-14:20 (describing example embodiment), 14:21-38 (describing example embodiments). Thus, the portion of the specification cited by the Court does not require Centripetal to prove that the traffic being analyzed is obfuscated. *Haddad v. United States*, 164 Fed. Cl. 28, 38 (2023)

(limitations from embodiments are not read into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited).

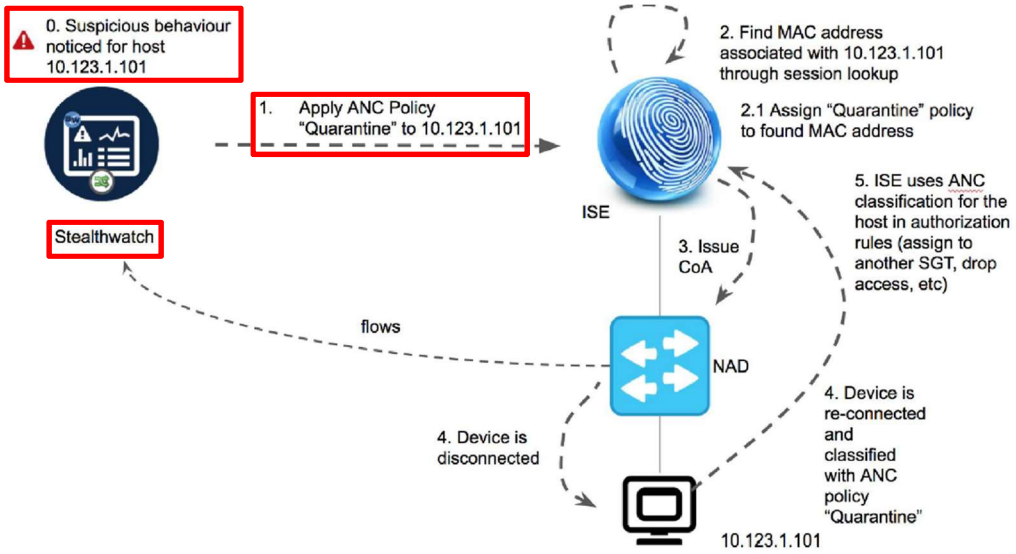
Without notice that the Court would narrow the plain meaning of the claims by appearing to require packet obfuscation as one of the limitations, Centripetal lacked any opportunity to present evidence that the Switches and Routers along with Stealthwatch infringe even under this interpretation. Centripetal can establish that they, can, in fact, be used to detect obfuscated traffic. *See* Declaration of Dr. Cole ("Cole Decl."), ¶¶ 5-9. For example, the accused products can perform functionality like Network Address Translation (or "NAT"), which will alter the packets, and can detect traffic entering and leaving other network devices that perform NAT. Cole Decl., ¶¶ 6-8. Cisco's expert confirmed that performing NAT is consistent with what is disclosed in the '176 Patent for altering packets. Tr. 2295:17-20. Accordingly, Centripetal should (at a minimum) be permitted to open the record to address this new claim construction provided by the Court in its Order.

B. The Court Erred in Concluding that the Accused Products Do Not Generate and Provision Rules in Response to Correlation

The Court erred in concluding that Stealthwatch does not "generate[], based on the correlating, one or more rules configured to identify packets received from the host located in the first network" or "provision[] a device" with those rules. Op.60.

First, Stealthwatch generates a "rule" as the claims require when it creates a policy update to initiate the quarantine. Op.60. The *Markman* order adopted the parties' agreed construction that a rule is "a condition or set of conditions that when satisfied cause a specific function to occur." Dkt.202 at 9. Stealthwatch generates a policy update that meets this construction because it includes a condition in the IP address of the host computer that will cause the function of quarantining a host computer. PTX-1089 at .1238 (showing "Quarantine"

function is applied to packets with the condition of having IP Address 10.123.1.101). Neither party disputes that the policy update causes the quarantining of a suspicious host. This is shown in the figure below, where Stealthwatch applies the policy for quarantine to a host exhibiting "suspicious behavior":



PTX-1089 at .1238 (red annotations added). The classification that the ISE generates in response to the policy generated by Stealthwatch is shown as "#5" in the above image. In its Order, the Court suggested that the ISE-generated classification is actually the rule, but the operation of the ISE is irrelevant to whether Stealthwatch generates a rule. *See* Op.60. The policy Stealthwatch generates is this same rule because this policy is what is applying the "quarantine" to the host. Furthermore, the policy includes the actual directions on how to perform the quarantine. PTX-1089 at .1238 (stating that "ISE uses ANC classification . . .").

In pointing to the actions of a human administrator for its non-infringement findings, the Court again misstated the operation of the Stealthwatch. Op.60. The undisputed evidence shows that Stealthwatch meets all the claim elements because it automatically generates the rule in response to the correlating of NetFlow and then propagates the responsive rule; the user just needs to click a button to approve the quarantine. Tr. 1000:2-1007:19, 2187:25-2188:5 (user

"clicks the quarantine button in the user interface . . ."); PTX-595 at 179; PTX-1089 at .1238. The automatic quarantining of a host by Stealthwatch appears in the upgraded Stealthwatch 7.0, which added the "Change Mitigation Actions" using policy updates to initiate quarantines. Tr. 1000:2-1007:19; PTX-595 at 179; PTX-1089 at 1238. The only human interaction required is the trivial task of clicking the button, and Stealthwatch performs all aspects of generating a rule and provisioning that rule. Furthermore, Judge Morgan's *Markman* Order supports this understanding that an administrator (the "user" of the system) can be enabled to approve the quarantine policy, where the Court rejected Cisco's argument that the "correlate" element excluded "user-defined filters or rules." Dkt.202 at 19-20.

Similarly, the Court's conclusion that there was no evidence that the generated rules would block packets again contradicts the record and is not grounds for a finding of non-infringement. In particular, the policies are designed to quarantine the host identified due to the correlation—as seen above in PTX-1089, where the particular IP address (a specific host) is quarantined. Tr. 1002:11-18, 1005:7-15; PTX-595 at 179; PTX-1089 at .1238; Dkt.725 (Centripetal's FoF/CoL) at ¶¶ 375-376 (FoF) (describing sending the policy for quarantine). Cisco's expert also confirmed this was the case at the Rule 63 hearing, where he stated that a quarantine rule could block all traffic based on the source. R.63 Tr. 154:7-11. The Court does not address this evidence that establishes this element is met.

CONCLUSION

For any and all of the foregoing reasons, Centripetal's Motion should be granted.

Respectfully submitted,

Dated: January 8, 2024

By: */s/ Stephen E. Noona*
Stephen Edward Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.

150 W. Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Paul J. Andre (*pro hac vice*)
Lisa Kobialka (*pro hac vice*)
James Hannah (*pro hac vice*)
Hannah Lee (*pro hac vice*)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
hlee@kramerlevin.com

ATTORNEYS FOR PLAINTIFF CENTRIPETAL NETWORKS, LLC

CERTIFICATE OF SERVICE

I hereby certify that on January 8, 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will automatically send notification of electronic filing to counsel of record.

/s/ Stephen E. Noona
Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com